Acta Montanistica Slovaca
ISSN 1335-1788
actamont.tuke.sk

The Secure Cyber Environment as a Determinant of Progress in Achieving ESG Compliance: A Global View

Junzhen ZHANG[1], Hanna YAROVENKO[2], Serhiy LYEONOV[3,2] and Piotr GUTOWSKI[4]*

Authors' affiliations and addresses:
[1] School of Economics and Engineering, Huanghuai University, 76 Kaiyuan Road, 463000, Zhumadian, China.
e-mail: 535037083@qq.com

[2] Economic Cybernetics Department, Sumy State University, Kharkivska Str., 116, 40007, Sumy, Sumy Oblast, Ukraine.
e-mail: h.yarovenko@biem.sumdu.edu.ua

[3] Department of Applied Social Sciences, Silesian University of Technology, 26-28 Roosevelt Str., 41-800, Zabrze, Poland.
e-mail: serhiy.lyeonov@polsl.pl

[4] Institute of Management, University of Szczecin, Cukrowa Str., 8, 71-004, Szczecin, Poland.
e-mail: piotr.gutowski@usz.edu.pl

***Correspondence:**
Serhiy LYEONOV, Silesian University of Technology, 26-28 Roosevelt Str., 41-800, Zabrze, Poland
e-mail: serhiy.lyeonov@polsl.pl

Acknowledgement:
This work was performed within the framework of state budget research No 0124U000544 "Cybersecurity and digital transformations of the country's wartime economy: the fight against cybercrime, corruption and the shadow sector".

How to cite this article:
Zhang, J., Yarovenko, H., Lyeonov, S. and Gutowski, P. (2025). The Secure Cyber Environment as a Determinant of Progress in Achieving ESG Compliance: A Global View. *Acta Montanistica Slovaca*, Volume 30 (4), 994-1008

DOI:
https://doi.org/10.46544/AMS.v30i4.11

Abstract
Establishing a reliable and secure cyber environment that addresses modern challenges and threats in advancing Industry 4.0 and 5.0 is one of the top goals of sustainable development, according to the World Economic Forum. Providing a safe space minimises the risk of environmental disasters arising from cyberattacks on critical infrastructure. It plays an essential role in data protection, thereby increasing the trust of business and government organisations and enhancing their social responsibility. Protecting against fraud, information leaks, and massive cyberattacks is crucial to effective corporate governance and increased organisational transparency. This study aims to identify the correlation between ESG indicators and the essential components of the national cybersecurity framework. The empirical part of the study includes the analysis of data from 144 countries, where the implementation of cybersecurity and ESG practices has varied histories. The study used canonical analysis to assess the relationships between cybersecurity factors and environmental, social, and managerial factors. This study confirmed the existence of two-way effects between ESG factors and cybersecurity. Moreover, ESG factors are strongly associated with improvements in cybersecurity, highlighting the critical role of sustainable practices in protecting the digital environment. These results can serve as recommendations for integrating cybersecurity strategies into policies to achieve global ESG compliance.

Keywords
ESG; cyber security; cyber environment; sustainability; canonical correlation

© 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

Introduction

Achieving environmental, social, and corporate governance (ESG) goals is an integral part of sustainable development for both individual companies and countries in general. They aim to ensure environmental responsibility, social justice, and effective corporate governance, contributing to long-term economic growth and sustainability. Their analysis enables the determination of the extent to which the country meets modern requirements for sustainable development and what risks or opportunities may arise for investors and businesses. In this case, how could cybersecurity relate to ESG? Are some cybersecurity components influencing the achievement of ESG goals, or could the level of implementation of ESG standards improve a company's, an industry's, or an economy's cybersecurity? Theoretically, the interconnection between cybersecurity and the implementation of ESG standards can be explained along each ESG vector.

The first vector is environmental responsibility. Efficient cybersecurity solutions should minimise energy use and reduce the carbon footprint associated with data centres and IT infrastructure, i.e., implementing energy-efficient cybersecurity measures supports environmental sustainability goals. For instance, modern cybersecurity solutions, such as the Advanced Encryption Standard, are designed to support secure, energy-efficient decision-making. Another aspect of the interaction between cybersecurity and environmental protection initiatives is adopting green data centre practices, including implementing energy-efficient cybersecurity measures. The shift towards cloud computing and virtualisation has also contributed to energy efficiency in cybersecurity. Cloud service providers, such as Amazon Web Services and Microsoft Azure, implement robust cybersecurity measures while optimising resource allocation and energy use. By utilising cloud-based security solutions, companies can reduce the need for on-premises servers, thereby lowering energy consumption and carbon emissions.

The second vector is the social aspects of interaction. The protection of customer and employee data should be mentioned here. This is a primary objective for cybersecurity. Ensuring data privacy and safety is also a social responsibility that helps build trust and maintain a company’s reputation, fostering long-term customer relationships. An IBM study found that 78% of consumers say a company’s ability to keep their data private is extremely important (IBM, 2018), and the publication of Cyber Security Review presented data that 75% will not buy from a company if they don’t trust how their data is handled (Cyber Security Review, 2018).

The third component of ESG is Governance. Incorporating cybersecurity into governance frameworks ensures companies are prepared for and resilient against cyber threats, a critical component of overall risk management. Adhering to cyber security laws and regulations (e.g., GDPR, CCPA) is mandatory for legal compliance. Another component of good governance practice is transparency. Companies must be transparent about their cybersecurity practices and breaches. Transparency in cybersecurity practices aligns with the broader ESG goal of maintaining high standards of corporate governance and accountability to stakeholders. Companies increasingly must disclose their cybersecurity practices and incidents as part of their regulatory compliance. These disclosures ensure companies maintain high governance standards by being accountable and transparent about their cybersecurity practices and risks. By reporting on cybersecurity practices, companies demonstrate their commitment to protecting customer and stakeholder information, a critical aspect of good governance and social responsibility.

The intersection of cybersecurity and ESG implementation is a strategic necessity and a forward-thinking approach that addresses the multifaceted risks and opportunities in today's business environment. As cyber threats evolve and stakeholder expectations grow, integrating robust cybersecurity measures into ESG frameworks will be crucial for sustainable, responsible business operations.

Literature review

Considering the multifaceted nature of the ESG concept, as well as its interaction with cyber security in various areas, the existing scientific works in the scientific literature also demonstrate the breadth of topics that are investigated and which, in one way or another, testify to the possible connection of cyber security and ESG indicators both at the level of business entities and at the state level as a whole.

The research agenda established that the latest and most revolutionary technologies are promising for achieving sustainable development, but the pool of scientific publications is insufficiently covered and needs to be expanded to achieve ESG goals (Dadkhah et al., 2024). In addition, public interest in digital transformation issues has constantly grown since 2014 (Ponomarenko, Kovalov, and Melnyk, 2024). Also, the growth of Internet users worldwide, the introduction of 4G and 5G technologies, and the availability of ICT underscore the relevance of this problem across countries (Kigerl, 2013; Kuzior et al., 2022). Using bibliometric analysis, the authors of the study (Zámek and Zakharkina, 2024) identified seven clusters covering topics ranging from digital transformation and adaptive management to global political and economic strategies, further confirming the multifaceted nature of ESG concepts. Moreover, the issue of achieving ecological, social, and economic stability in war conditions is raised (Kuzior et al., 2023a; Lu et al., 2025).

Thus, it has been proven that strategic management is the driver of companies' digital transformations (Červinka, 2023), which, in turn, shape their electronic reputation (Chang and Ku, 2023). At the same time, a reliable cybersecurity system is more important than the rapid development of modern technologies, which became relevant after the COVID-19 pandemic (Kuzior et al., 2023b). Using panel threshold analysis, the authors confirmed a relationship among new business density, entrepreneurship, and the digital integration of individuals in EU countries from 2006 to 2020 (Nicolescu et al., 2024). The connection between the country's technological leadership, the development of information and communication technologies, and the flexibility of companies was also revealed (Sour, Maliki, and Benghalem, 2023; Yamin and Murwaningsari, 2023). The authors (Wang et al., 2024; Lin et al., 2023) indicate that digital technologies and corporate social responsibility positively affect corporate financial performance and predict that integrating digital technologies with sustainable development strategies can increase financial benefits. Although, in general, digital innovations increase business efficiency (Sarlab et al., 2024; Zvarikova et al., 2024), certain aspects of digitalization, such as digital procurement, may not affect companies' economic sustainability (Chytilová et al., 2024).

Another aspect of research concerns the impact of digital technologies on the environment. It has been shown that they contribute to reducing China's ecological footprint (Li, 2024). The authors analyzed the impact of artificial intelligence software development on the energy transition and concluded that this process can contribute to the transition to renewable energy (Yin, Wen, and Chang, 2023). On the other hand, the following scientists claim that improvements in digital transformation do not significantly affect the environment in OECD member countries (Melnyk et al., 2022).

A separate research vector investigates transformations in human behavioural patterns as a factor of stakeholder requirements to companies. The articles (Oe and Yamaoka, 2023; Odei Addo and Keelson, 2023) aim to quantify how people's behaviour and interactions in the digital space influence changes in their personal behavioural patterns in the physical natural environment. A distinct line of research (Androniceanu and Georgescu, 2023; Omarova et al., 2024) examines the personal attributes of cybersecurity and digitalisation. Others investigate the interaction of the human brain with the processes of forming new knowledge in systems (Njegovanović, 2023). The authors (Dunn Cavelty, Eriksen, and Scharte, 2023) propose conceptualizing cybersecurity as a fusion of technical challenges and human factors or as a social issue intertwined with technological complexities. The next researchers contend that, in addition to cyberattacks targeting vulnerabilities in information technology systems, a new type of cyber threat has emerged: social engineering attacks that exploit human vulnerabilities (Nifakos et al., 2021). Introducing the latest technologies contributes to the active development of digital literacy of company employees (Krajčík et al., 2023; Farkačová et al., 2023). As a result, it significantly improves working conditions and provides equal rights for the practice of various professions (Benchea and Ilie, 2023; Sahnouni and Benghebrid, 2023). The authors concluded that companies should encourage their employees to use the latest technologies (Porkodi et al., 2023). The article (Cramarenco, Burcă-Voicu, and Dabija, 2023) showed the impact of artificial intelligence on workers' personal and professional lives, particularly in light of numerous technological disruptions spurred by the recent pandemic, which are reshaping global labour markets.

Some authors (Mukhtarov et al., 2024; Seniutis et al., 2024) attempt to analyse the current state of digital innovation implementation in public administration and to categorize and examine the primary ethical concerns associated with the use of digital technologies in this area. For instance, three main ethical issues in this area: privacy, security, and data protection; transparency and accountability; and inclusion, accessibility, and non-discrimination (Pakhnenko and Kuan, 2023). In a series of publications (Androniceanu, 2023; Androniceanu, 2024), the author highlights the evidence of rapid and effective adoption of artificial intelligence applications across diverse sectors of public and private concern. It emphasizes the need for public investments, particularly to foster sustainable development within the public sector. Investments aligned with ESG goals reduce emigration by improving the quality of life in the host country, enhancing environmental protection, and promoting more transparent corporate governance (Zatonatskiy et al., 2024). Also, investing in ESG initiatives makes companies more attractive to investors (Horobet et al., 2024).

The following research direction concerns the implementation of transparency requirements, both in ESG practices and in the policy of ensuring financial market regulators' confidentiality and data security (Kozhushko, 2023; Liu, 2023). It applies to requirements for financial lending (Agboola, Adelugba, and Eze, 2023) and manipulation of accounting information (Bachtijeva, Tamulevičienė, and Tvaronavičienė, 2023). It is especially relevant for combating financial fraud in general (Filatova et al., 2023) and ensuring personal protection in particular (Yarovenko et al., 2023). Therefore, the growth of innovations in the financial industry through Fintech increases the trust of financial services consumers (DingYi et al., 2024; Polishchuk, 2023). Also, implementing artificial intelligence, such as Robo-advisory, facilitates the decision-making support processes of customers in banks (Piotrowski and Orzeszko, 2023). The study (Habib et al., 2024) concludes that financial constraints and financial reporting quality are channels through which ESG compliance reduces cash holdings, whereas ESG compliance increases cash holdings via idiosyncratic and systematic risk channels. Furthermore, the effect of ESG compliance on cash holdings is more significant in firms located in regions with lower ESG compliance.

Over the past three years, the average data breach cost in healthcare has increased by 53.3%, rising by more than USD 3 million compared to the average cost of USD 7.13 million in 2020 (IBM Security, 2023). As a result, there are many publications, for example, (Ninassi and Burrell, 2023; Pakhnenko and Pudło, 2023) related to cybersecurity in healthcare. It is worth noting the article by Graf and Burrell (2024), which provides strategic guidance for healthcare organizations to efficiently address and alleviate these challenges, aiding a smooth transition to the healthcare technology environment. The study (Wright, 2023) highlights the significant risk that cybercrime poses to patient safety, data security, and operational efficiency in healthcare logistics and supply chain management. This threat extends to the organization's reputation and financial stability, highlighting the need for healthcare companies to remain vigilant in detecting and mitigating such risks.

While research on the interconnection of cybersecurity and ESG has been growing, there are still notable gaps in scientific inquiry that warrant further investigation. There is a need for longitudinal studies examining the effects of cybersecurity practices on ESG performance, not only within individual companies but also across industries or countries (Aden Dirir, 2023; Chao and Di, 2024). There is a lack of comprehensive analyses of how cybersecurity investments translate into sustained improvements in environmental, social, and governance outcomes over time. While there is considerable research on the governance aspects of cybersecurity within ESG frameworks, there is relatively less focus on the social and environmental dimensions. More research is needed to understand how cybersecurity practices affect social factors, such as consumer privacy and workforce well-being, as well as ecological factors, including energy consumption and carbon emissions. And really, does that influence exist?

Material and Methods

The idea of this study is related to finding the answer to the research question regarding the relationship between cyber environment development and the achievement of countries' ESG goals. The following steps are required for its implementation.

In the *first stage*, it is necessary to pre-process the data. The input set will be checked for missing and null values to do this. If they are available, information recovery procedures will be applied using averaging, exponential smoothing, or other techniques to produce a high-quality data frame. This step also includes standardizing the observations using Z-score normalization, transforming them to a distribution with a mean of 0 and a standard deviation of 1. This procedure will allow us to unify the data scale, reduce the impact of deviations, improve convergence, and facilitate data processing and analysis in subsequent stages.

In the *second stage*, it is necessary to check the variables for the presence of multicollinearity. This procedure is essential for such a study because this phenomenon can lead to overestimating the model's parameters. Therefore, the presence of multicollinearity will require reduction. This procedure will be carried out by calculating the Variance Inflation Factors (VIFs) for each indicator. If the obtained VIF values equal 1, then the factor is not correlated with the others. If $1 < VIF \leq 5$, the correlation is moderate and not problematic. $VIF > 5$ indicates potential multicollinearity and warrants attention, while $VIF > 10$ signals its severity and requires reduction. Since it is crucial to interpret the results for further research, the best solution in the presence of multicollinearity in this case would be to exclude the relevant factor from the set of variables.

The *third stage* of this study will focus on identifying and evaluating the relationships between the development of the cyber environment and achieving ESG compliance. For its implementation, a canonical analysis will be carried out, allowing the identification of linear combinations of variables X and Y that are maximally correlated. The components of the National Cyber Security Index will serve as the left set of X. ESG indices will serve as the right set of Y factors, but for this study, we will use the environmental, social, and governance groups separately to monitor the specifics of the relationship with individual ESG goals.

Canonical analysis will allow us to get the following information. First, the canonical correlation between the two sets of variables will be determined, enabling a conclusion about the strength of the linear relationship between them. Its significance will be confirmed using the Chi-square test and corresponding *p*-values. Secondly, the factor structure will be determined for each variable from sets X and Y. This will help interpret the significance of each variable in its corresponding data set and select only those with the greatest impact, thereby assigning them greater weight. For the analysis of socioeconomic processes, it is sufficient to retain only those factors with $|weights| \geq 0.3$; in exceptional cases, retaining variables with $|weights| \geq 0.2$ is possible. Thirdly, the canonical coefficients will be calculated and used to construct the canonical variables. It will allow the construction of canonical regressions that consider the relationships between the cybersecurity environment and a particular ESG target.

Two sets of indicators were chosen for the implementation of this research. The first group consisted of 12 components of the National Cyber Security Index (NCSI): Cyber security policy development, Cyber threat analysis and information, Education and professional development, Contribution to global cyber security, Protection of digital services, Protection of essential services, E-identification and trust services, Protection of personal data, Cyber incidents response, Cyber crisis management, Fight against cybercrime and Military cyber

operations (e-Governance Academy Foundation, 2023). These indices help us understand the overall state of the country's cybersecurity and its readiness to meet the challenges of the digital age. They help assess the effectiveness of the national cyber security policy, its strategic planning and implementation, the availability of cyber threat analysis systems and mechanisms for exchanging information about them, and the level of education and training of cyber security specialists. The indices also make it possible to determine the level of participation of countries in international initiatives and cooperation with other countries in the field of cybersecurity, the effectiveness of measures to protect digital services, including the Internet and electronic government services, and the presence and development of electronic identification and trusted digital services for the security of electronic transactions. In addition, the indicators assess the level of protection of critical infrastructures from cyber threats in energy, transport, medicine, etc., the protection of personal data from unauthorized access and use, the effectiveness of the response to cyber incidents and their management, measures to prevent cybercrime and law enforcement in cyberspace, military strategies and cyber operations and the country's readiness to manage cyber crises and incidents that could have serious consequences.

The second group of variables is formed based on ESG indicators that identify the country's profile in three areas – Environmental, Social, and Governance (The World Bank, 2023). Environmental indicators assess the state of the country's environment, including levels of air and water pollution, the amount of atmospheric emissions, the efficiency of energy use, the impact of climate change, etc. These data are essential for assessing the country's environmental sustainability and its ability to preserve natural resources for future generations. Social indicators characterize various aspects of society's life, such as the quality of education, the availability of health care, poverty levels, and social inequality. They indicate the degree of inclusion and well-being of citizens and the effectiveness of social programs and support systems. Governance indicators assess the quality of management practices in the country, including the effectiveness of public administration, transparency of decision-making, the fight against corruption, the stability of the legal system, and the implementation of legislation. This direction is vital for ensuring the rule of law and stability, and stimulating economic development and the investment climate.

Results and discussion

In the *first stage* of the proposed methodology, the data set was created for 144 countries worldwide from 2018 to 2022. The number of countries and ESG indicators was determined during pre-processing of the input dataset. Based on this, a group of ESG factors comprised 25 environmental indicators, 18 social indicators, and 17 governance factors. Then, the input data array was standardized, allowing it to be brought to a comparable form.

In the *second stage*, VIFs were calculated for groups based on cybersecurity, social, governance, and environmental factors. No multicollinearity was found in the cybersecurity array. In other groups, there are multicollinear variables that were excluded from further research: environmental – CO_2 emissions (metric tons per capita), Cooling Degree Days, Land Surface Temperature, social – Cause of death, by communicable diseases and maternal, prenatal and nutrition conditions (% of total), Fertility rate, total (births per woman), Mortality rate, under-5 (per 1,000 live births), and government – Rule of Law: Estimate, Regulatory Quality: Estimate, Government Effectiveness: Estimate.

In the *third stage* of the proposed methodology, a canonical analysis was performed. All its results are based on the first canonical root, which is statistically significant and the largest across the three calculations. Table 1 shows the results for 2018 and 2022 on environmental and cyber indicators, including only those with |factor loadings| $\geq$ 0.3. However, several variables with a lower degree of structure were retained due to significant changes over time.

Thus, it was determined that there is a high correlation between the selected environmental factors and the components of the cybersecurity index for both periods ($0.6 \leq r < 0.8$). As a result, an increase in environmental factors is associated with an increase in the country's cybersecurity level and vice versa. The obtained coefficient of determination values indicate a moderate relationship among these variables. The significance of the obtained coefficients is confirmed by the high values of the Chi-square test ($\chi 2$ = 269.0663; $\chi 2$ = 270.4075), with p-values not exceeding 0.05 in both cases (p = 0.0000). The redundancy values for both sets indicate mutual influence, albeit not very strong. Namely, environmental variables account for 34.3287% (2018) and 35.0112% (2022) of the variability of cybersecurity indicators (Table 1). In turn, they only explain the variability of environmental factors by 20.7082% (2018) and 20.4760% (2022) (Table 1). This means that ecological variables are associated with cybersecurity, accounting for more than a third of its variation. Cybersecurity is also associated with environmental factors, but this influence is less significant. Over time (from 2018 to 2022), the impact of environmental variables on cybersecurity increased slightly, while the reverse impact decreased (Table 1). It indicates the asymmetric nature of the interaction between these variables, in which environmental factors significantly affect cybersecurity more than vice versa.

Tab. 1. Canonical analysis results for cyber security and environmental indicators

Variables and parameters of canonical analysis	2018		2022	
	FS*	CW*	FS*	CW*
Left Set				
Cyber security policy development	0.8035	0.2504	0.8296	0.3022
Cyber threat analysis and information	0.6858	-0.0410	0.6786	0.0257
Education and professional development	0.7772	0.1999	0.7824	0.1555
Contribution to global cybersecurity	0.5807	-0.0514	0.6869	0.0917
Protection of digital services	0.5279	0.0435	0.5524	-0.0114
Protection of essential services	0.6454	-0.0088	0.6207	-0.0308
E-identification and trust services	0.7237	0.1040	0.6222	-0.0688
Protection of personal data	0.6367	0.2068	0.6177	0.1933
Cyber incidents response	0.6422	0.1428	0.7742	0.3169
Cyber crisis management	0.6847	0.1281	0.7263	0.0614
Fight against cybercrime	0.8133	0.1703	0.8248	0.2816
Military cyber operations	0.7176	0.2218	0.6558	-0.0399
Variance extracted	100%		100%	
Total redundancy	34.3287%		35.0112%	
Right Set				
Adjusted savings: natural resources depletion	-0.5086	-0.1047	-0.5092	-0.1142
Agriculture, forestry, and fishing, value added	-0.7027	-0.2328	-0.6979	-0.2041
Energy imports, net	0.3095	0.2739	0.3311	0.3360
Energy intensity level of primary energy	-0.3380	-0.3370	-0.3366	-0.2884
Energy use	0.4295	0.4046	0.4715	0.4266
Food production index	-0.2359	-0.0704	-0.2810	-0.0060
Fossil fuel energy consumption	0.5414	0.4477	0.6478	0.5869
Heating Degree Days	0.5925	0.2410	0.4662	0.1478
PM2.5 air pollution	-0.4847	-0.1270	-0.4548	-0.0664
Renewable energy consumption	-0.3678	0.4560	-0.4001	0.3779
Standardised Precipitation-Evapotranspiration Index	-0.3608	-0.1861	0.2103	0.1432
Terrestrial and marine protected areas	0.3803	0.1261	0.3197	0.0938
Variance extracted	100%		100%	
Total redundancy	20.7082%		20.4760%	
Canonical Analysis Summary				
Canonical R	0.7905		0.7907	
Canonical R-sqr	0.6249		0.6252	
Chi^2	269.0663		270.4075	
p	0		0	

**FS – Factor Structure; CW – Canonical Weights.*

The analysis identified indicators with the highest factor loadings, such as Energy use (kg of oil equivalent per capita), Fossil fuel energy consumption (% of total), and Energy imports, net (% of energy use) (Table 1). They demonstrate a positive impact on the cyber environment, as the values of their canonical weights are positive. This result confirms that one of the key aspects of protection is energy stability, as a reliable power supply is critical for the functioning of cybersecurity systems, including servers, data centres, and other resources. Its absence or violation can make information systems vulnerable to attacks. On the other hand, Renewable energy consumption (% of total final energy consumption) negatively contributes to the formation of environmental factors (Table 1). It may be due to specific regional or contextual conditions that prevent us from fully experiencing the positive impact of renewable energy sources on the environment, as well as to differences in countries' policy approaches and varying levels of development. However, it has a relatively strong and positive effect on the formation of the canonical weight and, accordingly, on the creation of the security environment. That is, it provides a broader range of benefits that renewable energy sources have for national and global security, including energy independence, economic stability, and mitigation of externalities.

On the other hand, Adjusted savings: natural resources depletion (% of GNI), Agriculture, forestry, and fishing, value added (% of GDP), Energy intensity level of primary energy (MJ/$2017 PPP GDP), PM2.5 air pollution, mean annual exposure (micrograms per cubic meter) and Standardized Precipitation-Evapotranspiration Index (for 2018) reduce the potential for cyber development, as they have a negative impact on a combination of environmental and cyber security factors (Table 1). That is, changes in ecology (for example, global warming, environmental pollution, violation of temperature regimes, etc.) can lead to a breach of ecological stability in the design, deployment, and management of information systems, which ultimately can cause risks of cyber attacks, deterioration of information infrastructure, or a decrease in the level of system security. A high level of energy intensity can indicate outdated infrastructure and technology, which is not conducive to the development of cyberspace and innovation. High levels of air pollution indicate poor environmental health, which can limit investment in cyberinfrastructure as resources are diverted to addressing environmental problems and ensuring public health. Climate change can lead to extreme weather conditions that can destroy infrastructure, including cyber infrastructure, and divert resources from development to disaster relief. The large share of agriculture, forestry, and fishing in GDP may indicate that the economy is heavily dependent on the primary sector, which inhibits technological development and cybersecurity.

The analysis of factor structure and canonical weights for the components of cyber security revealed that the most significant for the environmental direction are Cyber security policy development, Education and professional development, Protection of personal data, Cyber incidents response, Fight against cybercrime, Cyber crisis management (2018), and Military cyber operations (2018) (Table 1). Developing a cybersecurity policy contributes to the stability of ecological systems by reducing the risk of environmental disasters caused by cyberattacks, infrastructure disruptions, water management systems, or energy networks. Improving cybersecurity professionals' skills and awareness helps better prepare for potential threats and minimize risks and their corresponding consequences. An effective response to cyber incidents enables the rapid restoration of the operation of ecologically important systems after attacks, minimizing their negative environmental impact. Managing cyber crises is critical to preventing or minimizing their ecological consequences, ensuring operational coordination, and responding to threats. Military cyber operations can protect against cyber threats targeting environmental targets. However, uncontrolled use of cyber weapons can lead to ecological disasters if attacks target critical infrastructure such as water supplies, power grids, or hazardous materials plants. In general, these aspects can significantly enhance the protection and resilience of ecological systems and minimize the risks and adverse environmental effects of cyber threats. As for other factors, they account for more than 50% of those that form the cyber environment but have a weak impact on achieving environmental goals.

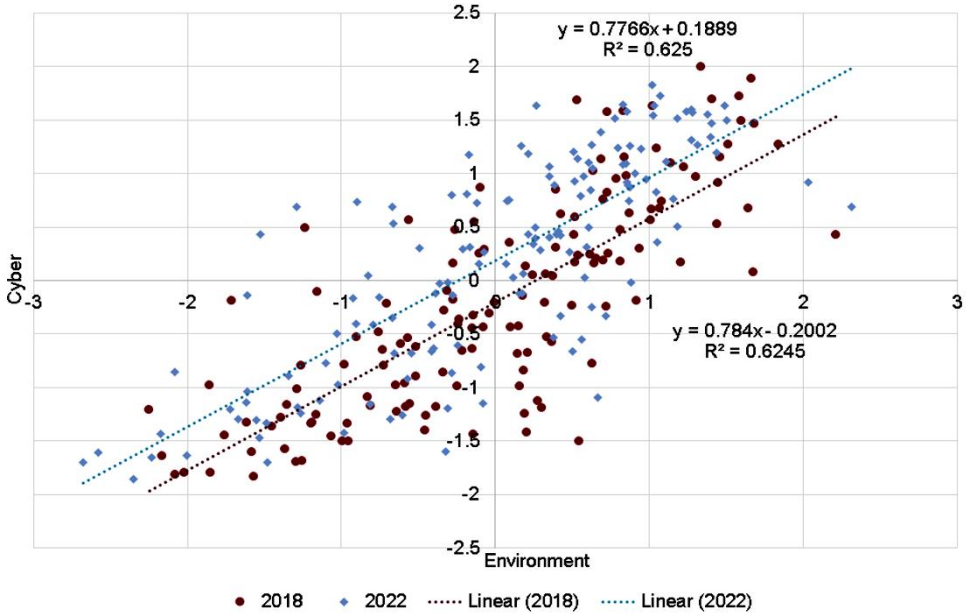

Fig. 1. Canonical Correlation Plot between environmental and cyber variables

Canonical weights were used to construct the Canonical Correlation Plot between environment and cyber variables (Figure 1). Figure 1 shows the distribution and clustering of most values in the first and third quadrants of the coordinate plane, indicating the symmetry of the obtained values. It can be seen that countries with a high level of cybersecurity have the highest weighted total value of the group of environmental indicators, which characterizes them as countries with a high potential for creating a reliable cyber environment and conditions for

improving the environment. Countries with low cybersecurity are concentrated in the third quadrant, which is also characterized by low environmental development.

Table 2 presents the results for the selected social and cyber factors, with a threshold of significance ≥ |±0.3|. It was established that there is a very high positive correlation between social and cybersecurity factors for both periods ($r \geq 0.8$). The coefficient of determination values confirm a moderate relationship in this set of variables, 69.85% (2018) and 63.41% (2022) of the total variation, which in one set is explained by the total variation in the other. The statistical significance of the obtained coefficients is confirmed by the Chi-square statistic, with a significance level below 0.05 (Table 2).

Tab. 2. Canonical analysis results for cyber security and social indicators

Variables and parameters of canonical analysis	2018		2022	
	FS*	CW*	FS*	CW*
Left Set				
Cyber security policy development	0.7362	0.0761	0.7327	0.0581
Cyber threat analysis and information	0.7314	0.1665	0.7474	0.1626
Education and professional development	0.6531	-0.0613	0.6572	-0.1285
Contribution to global cybersecurity	0.6206	0.0110	0.7514	0.2103
Protection of digital services	0.6324	0.1656	0.7045	0.2033
Protection of essential services	0.7203	0.1481	0.6848	0.0768
E-identification and trust services	0.6580	-0.0083	0.6367	0.0046
Protection of personal data	0.6837	0.3214	0.6420	0.2473
Cyber incidents response	0.5899	0.1158	0.7234	0.1746
Cyber crisis management	0.6015	-0.0149	0.7054	0.0070
Fight against cybercrime	0.7571	0.1437	0.7374	0.1050
Military cyber operations	0.7615	0.3434	0.7676	0.2555
Variance extracted	100%		100%	
Total redundancy	38.0946%		37.2164%	
Right Set				
Access to clean fuels and technologies for cooking	0.5817	0.1894	0.6439	0.1552
Access to electricity	0.4899	-0.0227	0.5664	0.0114
Government expenditure on education, total	-0.2929	-0.0521	-0.3547	-0.0468
Hospital beds	0.5914	-0.1233	0.5802	-0.1941
Income share held by the lowest 20%	0.3497	0.1083	0.3385	0.1217
Labor force participation rate, total	0.5013	0.1849	0.5370	0.2079
Life expectancy at birth, total	0.7409	0.0459	0.8061	0.0956
Literacy rate, adult total	-0.4061	-0.0864	-0.2746	0.0163
Population ages 65 and above	0.9666	0.8249	0.9573	0.7753
Poverty headcount ratio at national poverty lines	-0.3610	0.0886	-0.4570	0.0457
Prevalence of overweight	0.4741	0.0107	0.5371	0.0324
Prevalence of undernourishment	-0.4755	0.0242	-0.5887	-0.0434
Variance extracted	100%		100%	
Total redundancy	28.5931%		29.2952%	
Canonical Analysis Summary				
Canonical R	0.8358		0.7963	
Canonical R-sqr	0.6985		0.6341	
Chi^2	308.4706		295.4694	
p	0		0	

**FS – Factor Structure; CW – Canonical Weights.*

The redundancy values for both sets indicate a mutual relationship between the variables. Thus, social factors account for 38.0946% (2018) and 37.2164% (2022) of the variability of cybersecurity indicators, which, in turn, explain 28.5931% (2018) and 29.2952% (2022) of the variability of social spheres (Table 2). The two-way

relationship between the factors over time is asymmetric, indicating that cybersecurity explains an increasing share of the variation in social indicators.

The positive influence on cyberspace through the formation of a favourable social environment is carried out by Access to clean fuels and technologies for cooking (% of population), Income share held by the lowest 20%, Labor force participation rate, total (% of total population ages 15 - 64), Life expectancy at birth, total (years), Population ages 65 and above (% of total population) (Table 2). Generally, longer life expectancy indicates solid development and stability in developed countries. Accordingly, such countries have a strong potential for more effective protection of cyberspace. Also, the economically active population contributes to the development of cybersecurity through work in relevant IT sectors. Population demographics can significantly impact cybersecurity, as older populations may have specific cybersecurity needs or their presence may influence overall policies and strategies in this area. High income among the poorest 20% of the population points to less economic inequality, which contributes to social stability, access to education, and opportunities for development, including cyber education. Access to clean cooking fuels and technologies means the population has better living and health conditions, as household air pollution is reduced. It contributes to improving general welfare and advancing social standards. Countries with higher levels of social development tend to demonstrate higher levels of cyber protection.

Cyber threat analysis and information, Protection of digital services, Protection of essential services, Protection of personal data, Cyber incident response, Military cyber operations, and the Fight against cybercrime proved critical to the cyber sphere (Table 2). Effective protection of personal data increases citizens' trust in digital services and government systems, promotes more active use of digital services, and improves access to education, health care, and other vital services, ultimately increasing the population's well-being. Protecting digital services ensures the uninterrupted operation of online platforms, which is essential for business and economic activity and contributes to creating new jobs and economic growth. The growth of analytical capabilities helps disseminate information among the population. It increases its level of cyber literacy, which contributes to preventing cybercrimes and forming a safe digital culture. Reliable protection of critical services (energy, transport, health care, etc.) ensures the stability and continuity of their operations, which are essential to citizens' everyday lives and to society's functioning. Also, a high level of military cyber operations ensures the protection of the country's national infrastructure and its security, which affects the formation of an environment for social and economic development. An effective fight against cybercrime increases the level of security and citizens' trust in digital technologies, reducing the risks and consequences of criminal activity in cyberspace.

Also, the growth in the importance of contributions to global cybersecurity should be noted for 2022 (Table 2). It may be related to a change in the trajectory of cybersecurity strategies, reorienting them at the global level, as evidenced by the increase in Contributions to international cybersecurity. This result may be a consequence of sustainable development strategies, in which cybersecurity is a top priority for the near future. The global COVID-19 pandemic also had a significant impact, leading to increased cybercrime and overall crime levels.

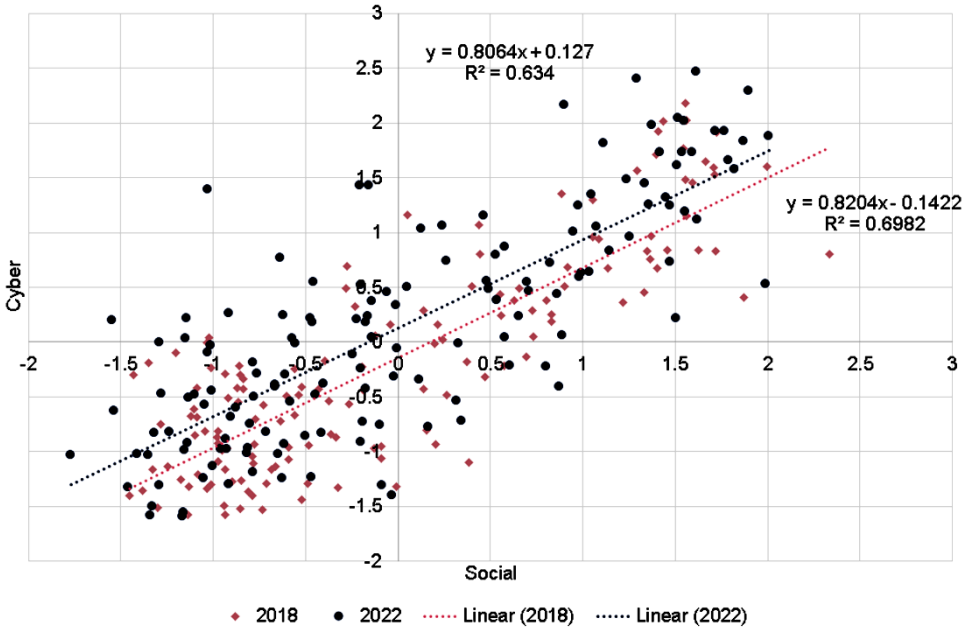

Fig. 2. Canonical Correlation Plot between social and cyber variables

The results of the canonical analysis enabled the construction of a Canonical Correlation Plot between social and cyber variables (Figure 2). Chart 2 shows a significant density of the distribution of results in the third quadrant

of the coordinate plane. The first quartile also has a cluster of values, but its density indicates the presence of different country variations. There are no critical anomalies on the chart and a visible trend with a good level of approximation. In general, the points are symmetrically distributed around the origin, which allows us to draw the following conclusion. The highest weighted total value of the group of social indicators also characterizes countries with a high-weighted total level of cybersecurity. Conversely, countries with low levels of cybersecurity development have relatively low levels of social development. This conclusion is confirmed for both analyzed periods.

Table 3 shows the results for the governance and cybersecurity factors. As a result, a very high positive correlation between the governance and cybersecurity factors was revealed ($r \geq 0.8$). The coefficient of determination confirms a relatively strong connection for these factors, 71.66% (2018), and a moderate one, 73.95% (2022). The statistical significance of the obtained coefficients is confirmed by the Chi-square test (χ^2 = 282.5524; χ^2 = 259.1554), and the significance level is less than 0.05.

Tab. 3. Canonical analysis results for cyber security and governance indicators

Variables and parameters of canonical analysis	2018		2022	
	FS*	CW*	FS*	CW*
Left Set				
Cyber security policy development	0.7821	0.2216	0.7011	0.0124
Cyber threat analysis and information	0.7260	0.1453	0.7412	0.1435
Education and professional development	0.7441	0.2095	0.7166	0.0157
Contribution to global cybersecurity	0.7322	0.2065	0.8086	0.3162
Protection of digital services	0.4427	-0.0626	0.5531	0.0376
Protection of essential services	0.5839	-0.0259	0.5800	0.0018
E-identification and trust services	0.5870	-0.0595	0.5351	-0.1194
Protection of personal data	0.6914	0.3721	0.6914	0.3518
Cyber incidents response	0.5370	0.0937	0.6421	0.1494
Cyber crisis management	0.5822	-0.0476	0.7015	0.0252
Fight against cybercrime	0.7349	0.0058	0.7467	0.1249
Military cyber operations	0.7447	0.2790	0.7839	0.2677
Variance extracted	82.4845%		83.0244%	
Total redundancy	36.3046%		35.2826%	
Right Set				
Control of Corruption: Estimate	0.7546	-0.0755	0.7608	-0.0787
Economic and Social Rights Performance Score	0.5276	0.0926	0.5821	0.0939
Individuals using the Internet	0.8009	0.5733	0.7913	0.5071
Net migration	0.3137	-0.0308	0.2886	-0.0345
Political Stability and Absence of Violence/Terrorism: Estimate	0.4933	-0.3590	0.5509	-0.2570
Ratio of female to male labor force participation rate (%)	0.2495	0.1561	0.2878	0.1163
Research and development expenditure	0.8549	0.4301	0.8311	0.4442
Voice and Accountability: Estimate	0.7558	0.4354	0.7848	0.4495
Variance extracted	100%		100%	
Total redundancy	34.6957%		34.0447%	
Canonical Analysis Summary				
Canonical R	0.8465		0.8106	
Canonical R-sqr	0.7166		0.6570	
Chi²	282.5524		259.1554	
p	0		0	

**FS – Factor Structure; CW – Canonical Weights.*

The redundancy values for both sets indicate a mutual relationship. Thus, governance factors explain the variability of cybersecurity indicators by 36.3046% (2018) and 35.2826% (2022), which explains the variability of the governance sphere by 34.6957% (2018) and 34.0447% (2022) (Table 3). This conclusion stems from the close association between the country's management strategies and its cyber defence strategies, especially in recent years. This is due to the speed of implementation of Industry 4.0 and the consequences of Industry 5.0 across

various spheres of social life, the growth of cyber threats and cyber wars, the digitalization of society, and other challenges.

Individuals using the Internet (% of population), Ratio of female to male labour force participation rate (%) (modelled ILO estimate), Research and development expenditure (% of GDP), and Voice and Accountability: Estimates are the most weighted variables (Table 3). The growth in Internet users underscores the need for robust cybersecurity to protect personal data and digital services. It encourages the development of appropriate cybersecurity policies and practices. In addition, R&D spending drives innovation, including new technologies that improve the reliability and effectiveness of cybersecurity for government, business, and the public. Also, open access to information increases citizens' awareness of personal cyber protection and prompts companies to change management strategies to protect data and counter threats. In addition, freedom of expression facilitates the exchange of information about cyber threats and the coordination of efforts to neutralize them. Equality in the workforce can lead to more innovative approaches in cybersecurity, as the inclusion of women in the industry promotes diversity of thought and decision-making. Ensuring educational, economic, and social rights increases well-being, social stability, digital literacy, and awareness of cyber threats, which helps citizens better protect themselves in cyberspace.

Control of Corruption: Estimate and Political Stability and Absence of Violence/Terrorism: Estimates demonstrate a significant weight for the governance factors and a significant negative impact on the canonical variable (Table 3). Quality control over corruption reduces opportunities for abuse of power and ensures the fair implementation of laws and policies, which is essential for implementing good governance. At the same time, the fight against this phenomenon helps identify vulnerabilities in information structures and systems, which can temporarily increase cyber risks by opening new channels for cybercriminal attacks. As for the stability of the political system and the absence of violence, the creation of favourable conditions for their provision is a consequence of effective management by state bodies. In such an environment, a re-evaluation of priorities is possible, in which attention to cybersecurity may decrease as governments and organizations direct resources to improve the governance framework for stability in politics, the economy, and society.

Cyber threat analysis and information, Contribution to global cyber security, Protection of personal data, Cyber incidents response, and Military cyber operations are essential components of cyber security (Table 3). Others also show promising results within the framework of a single analyzed year, for example, Cybersecurity policy development (2018), Education and professional development (2018), and the Fight against cybercrime (2022). These results indicate that most components of cybersecurity are essential for developing governance. Thus, informed decision-making in the field of cybersecurity is associated with higher levels of security and management stability. Strengthening international trust and cooperation helps improve management practices and counter cyber threats at the state level. Ensuring the confidentiality of information increases citizens' trust in government bodies and contributes to the legitimacy of management processes. Operational management of crises, defence preparedness, and response to cyber-aggressions increase the level of preparedness and response of states to cyber threats.

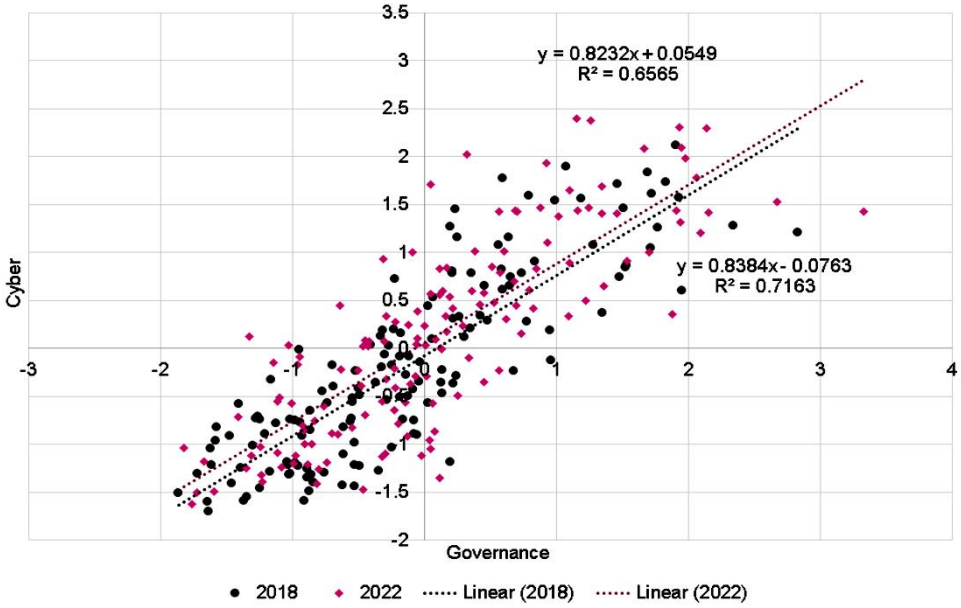

Fig. 3. Canonical Correlation Plot between governance and cyber variables

he calculations made it possible to build a Canonical Correlation Plot between government and cyber variables (Figure 3). Canonical Correlation Plot 3 demonstrates a symmetrical, relatively dense distribution of canonical variable results in the first and third quadrants of the coordinate plane. There are no critical anomalies. The figure clearly shows a trend with a good level of approximation. The obtained results allow us to draw the conclusion that countries with a high-weighted total level of cybersecurity are also characterized by the highest weighted total value of the group of government indicators, and vice versa. This trend is typical for both periods.

Conclusion

This study was conducted to identify relationships between ESG indicators and critical components of national cybersecurity. The results of the canonical analysis showed that there are strong, statistically significant relationships between the indicators that determine the country's cyber environment and sets of environmental, social, and governance factors. It means that improvement in one area is associated with improvement in another. At the same time, the nature of this relationship is not coincidental, underscoring the importance of considering ESG factors in developing and implementing cybersecurity policies. Conversely, when ESG requirements are met, one potential direction for improvement should be measures to establish a secure cyber environment for companies, users, and government agencies.

The results demonstrated that ESG factors explain approximately 34.3287% to 38.0946% of the variation in cyberspace, while cybersecurity measures explain approximately 20.4760% to 34.6957% of the variation in ESG targets. It shows a relatively significant level of influence, given the nature of the analyzed spheres. At the same time, environmental, social, and governance factors account for a greater share of variation in cybersecurity than the other way around. Moreover, a vital role in forming a secure cyberspace among ESG requirements is strongly associated with factors related to energy stability, an economically active population, a high standard of living, clean fuels and technologies, gender and income equality, democratic rights, and the corresponding level of scientific research and technology.

Integrating ESG indicators into cybersecurity policies can enhance the overall resilience and security of the cyber environment, thereby contributing to sustainable development at the global level. It will achieve the following key benefits. Including ESG indicators in the cybersecurity strategy will help create a comprehensive approach that considers not only the technical aspects of protection but also social and ethical requirements. Companies that demonstrate high standards of ESG and cybersecurity are more attractive to investors and competitive, which can attract new customers. Their compliance will help avoid legal sanctions and reduce risks from cyber incidents, thereby building a reliable and sustainable reputation. Also, such companies receive government support, which will ultimately enable the active development of policies to support sustainable development and cybersecurity.

On the other hand, the obtained results can serve as recommendations for integrating cybersecurity strategies into policies to achieve compliance with ESG requirements. Implementing cybersecurity measures in the context of ESG will demonstrate the commitment of companies and government organizations to act in the public interest, protecting both digital and physical infrastructure, showing responsibility for the environment, and avoiding environmental disasters that cyber threats can cause. Ensuring cybersecurity as part of ESG requirements will increase transparency in business processes, prevent reputational losses from information leaks and cyberattacks, improve management processes, and enhance organizational effectiveness.

References

Aden Dirir, S. (2023). The potential of macroeconomic factors in shaping the landscape of technological development: a testimonial from upper-middle-income countries. Business, Management and Economics Engineering, 21(1), 84–105.

Agboola, O., Adelugba, I. A., and Eze, B. U. (2023). Effect of financial technology on the survival of micro-enterprises. International Journal of Entrepreneurial Knowledge, 11(1), 1–13.

Androniceanu, A. (2023). The new trends of digital transformation and artificial intelligence in public administration. Administratie si Management Public, 40, 147–155.

Androniceanu, A. (2024). Artificial intelligence in administration and public management. Administratie si Management Public, 42, 99–114.

Androniceanu, A., and Georgescu, I. (2023). Digital competences and human development: a canonical correlation analysis in Romania. Polish Journal of Management Studies, 28(1), 43–61.

Bachtijeva, D., Tamulevičienė, D., and Tvaronavičienė, M. (2023). Do socially responsible companies use earnings management more rarely and (or) less aggressively? Evidence from Lithuania. Journal of International Studies, 16(4), 9–26.

Benchea, L., and Ilie, A. G. (2023). Preparing for a new world of work: Leadership styles reconfigured in the Digital age. European Journal of Interdisciplinary Studies, 15(1), 135–143.

Chang, K.-Y., and Ku, E. C. S. (2023). Discount or Prestige: E-reputation, Compatibility, and Continued Mobile Apps Usage Intention of Low-Cost Carriers. Journal of Tourism and Services, 14(26), 73–91.

Chao, L., and Di, L. (2024). Comparative Analysis of Digitalization and Economic Growth and Relevant Countermeasures. Transformations in Business and Economics, 23(1), 196–214.

Červinka, T. (2023). Digital Transformation of strategic management of SMEs in the Czech Republic. European Journal of Interdisciplinary Studies, 15(1), 144–155.

Cramarenco, R. E., Burcă-Voicu, M. I., and Dabija, D. C. (2023). The impact of artificial intelligence (AI) on employees' skills and well-being in global labor markets: A systematic review. Oeconomia Copernicana, 14(3), 731–767.

Cyber Security Review. (2018). Cyber Security Review. Available at: https://www.cybersecurity-review.com/75-of-consumers-wont-buy-your-product-if-they-dont-trust-you-to-protect-their-data/.

Dadkhah, M., Nedungadi, P., Raman, R., and Dénes Dávid, L. (2024). Emerging and disruptive technologies and the sustainable development goals: A state of art and research agenda. Equilibrium. Quarterly Journal of Economics and Economic Policy, 19(1), 13–21.

DingYi, W., Yamaoka, Y., Sartamorn, S., and Oe, H. (2024). Can citizen Internet banking in China become a champion in the digital transformation era? Financial Markets, Institutions and Risks, 8(1), 16–30.

Dunn Cavelty, M., Eriksen, C., and Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. Journal of Risk Research, 26(7), 801–814.

e-Governance Academy Foundation. (2023). National Cyber Security Index. Available at: https://ncsi.ega.ee/ncsi-index/.

Farkačová, L., Zadražilová, I., Tomášková, A., et al. (2023). A multi-criteria model approach to extended information literacy as a basis of labour market sustainability in V4 countries. Polish Journal of Management Studies, 28(2), 91–107.

Filatova, H., Tumpach, M., Reshetniak, Y., Lyeonov, S., and Vynnychenko, N. (2023). Public policy and financial regulation in preventing and combating financial fraud: a bibliometric analysis. Public and Municipal Finance, 12(1), 48–61.

Graf, D. G., and Burrell, D. N. (2024). Utilising resistance feedback for software implementation in healthcare. Health Economics and Management Review, 5(1), 106–116.

Habib, A., Khan, M. A., Popp, J., and Tangl, A. (2024). Does ESG Compliance Manipulate the Different Channels of Cash Holding? Montenegrin Journal of Economics, 20(1), 185–196.

Horobet, A., Bulai, V., Radulescu, M., Belascu, L., and Dumitrescu, D. G. (2024). ESG actions, corporate discourse, and market assessment nexus: evidence from the oil and gas sector. Journal of Business Economics and Management, 25(1), 153–174.

IBM. (2018). The Significant Gap Between Data Privacy and Consumer Trust. Available at: https://newsroom.ibm.com/IBM-security?item=30435.

IBM Security. (2023). Cost of a Data Breach Report 2023. Available at: https://www.ibm.com/downloads/cas/E3G5JMBP.

Kigerl, A. (2013). Infringing nations: Predicting software piracy rates, BitTorrent tracker hosting, and p2p file sharing client downloads between countries. International Journal of Cyber Criminology, 7(1), 62.

Kozhushko, I. (2023). Transformation of Financial Services Industry in Conditions of Digitalization of Economy. Financial Markets, Institutions and Risks, 7(4), 189–200.

Krajčík, V., Novotný, O., Civelek, M., and Semrádová Zvolánková, S. (2023). Digital Literacy and Digital Transformation Activities of Service and Manufacturing SMEs. Journal of Tourism and Services, 14(26), 242–262.

Kuzior, A., Kostenko, A., Sotnyk, I., Chortok, Y., Tuliakov, O., and Podmanicka, M. (2023a). Socioeconomic Sustainability and the Solidarity Economy Formation under the war conditions in Ukraine. Financial and Credit Activity Problems of Theory and Practice, 5(52), 256–267.

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., and Brożek, P. (2022). Global Digital Convergence: Impact of cybersecurity, Business Transparency, economic transformation, and AML efficiency. Journal of Open Innovation: Technology, Market, and Complexity, 8(4), 195.

Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., and Vasilyeva, T. (2023b). Company cybersecurity system: Assessment, risks and expectations. Production Engineering Archives, 29(4), 379–392.

Li, P. (2024). Digital Technologies, environmental governance and environmental performance: Empirical evidence from China. Engineering Economics, 35(2), 236–248.

Lin, W., Wang, Y., Samara, G., & Lu, J. (2024). Governance of corporate social responsibility: a platform ecosystem perspective. Management Decision, 62(12), 3782-3816.

Liu, K. (2023). Shanghai Stock Exchange's Science and Technology Innovation Board: A Review. Financial Markets, Institutions and Risks, 7(1), 1–15.

Lu, J., Rong, D., Eweje, G., Yuan, X., Song, M., & Searcy, C. (2025). Effective environmental strategy or illusory tactics? Corporate greenwashing and innovation willingness. Business Strategy and the Environment, 34(1), 1338-1356.

Melnyk, L., Kubatko, O., Piven, V., Klymenko, K., and Rybina, L. (2022). Digital and economic transformations for Sustainable Development Promotion: A case of OECD countries. Environmental Economics, 12(1), 140–148.

Mukhtarov, S., Aliyev, J., Jabiyev, F., and Aslan, D. H. (2024). The role of institutional quality in reducing environmental degradation in Canada. Economics and Sociology, 17(1), 89–102.

Nicolescu, A.-C., Lobonț, O.-R., Vătavu, S., and Bozga, E. (2024). Entrepreneurship and digitalisation in EU: twinning insights through a panel threshold regression. Journal of Business Economics and Management, 25(2), 315–336.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., and Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors, 21(15), 5119.

Ninassi, C. J., and Burrell, D. N. (2023). Teaching business leadership skills to professionals in healthcare cybersecurity, biodefense and biotechnology through experiential learning methods. Health Economics and Management Review, 4(3), 82–94.

Njegovanović, A. (2023). Quantum Entanglement of the Brain, Dynamics of Information, and Intelligent Finance. Financial Markets, Institutions and Risks, 7(3), 12–30.

Odei Addo, J., and Keelson, S. A. (2023). Moderating role of the media in celebrity endorsement and product adoption. International Journal of Entrepreneurial Knowledge, 11(2), 109–126.

Oe, H., and Yamaoka, Y. (2023). The impact of the digital environment on eco-friendly behavioural change towards nature: Exploring the concept of forest bathing without forest. SocioEconomic Challenges, 7(3), 76–93.

Omarova, A., Niyazov, M., Turekulova, A., Turekulova, D., Mukhambetova, L., and Mukhambetov, Y. (2024). Socioeconomic Development of Youth Policy in the Context of Digital Transformation. Montenegrin Journal of Economics, 20(1), 197–208.

Pakhnenko, O., and Kuan, Z. (2023). Ethics of Digital Innovation in Public Administration. Business Ethics and Leadership, 7(1), 113–121.

Pakhnenko, O., and Pudło, T. (2023). HealthTech in ensuring the resilience of communities in the post-pandemic period. Health Economics and Management Review, 4(2), 31–39.

Piotrowski, D., and Orzeszko, W. (2023). Artificial intelligence and customers' intention to use robo-advisory in banking services. Equilibrium. Quarterly Journal of Economics and Economic Policy, 18(4), 967–1007.

Polishchuk, Y. (2023). Fintech future trends. The European Digital Economy, 204–220.

Ponomarenko, I., Kovalov, B. L., and Melnyk, M. (2024). Business Innovations and Digital Transformation: Trend, Comparative and Bibliometric Analysis. Business Ethics and Leadership, 8(1), 74–92.

Porkodi, S., Al Balushi, S. S., Al Balushi, M. K., Al Hadi, K. O., and Al Balushi, Z. I. (2023). Digital employee experience and organizational performance: A study of the telecommunications sector in Oman. Business, Management and Economics Engineering, 21(2), 248–268.

Sahnouni, M., and Benghebrid, R. (2023). Competency Assessment Based on Fuzzy Logic and Artificial Intelligence Mechanism: A Study of Competency Assessment Document for the Algerian SEROR Company. Business Ethics and Leadership, 7(4), 159–170.

Sarlab, R., Rostamzadeh, R., Saparauskas, J., and Turskis, Z. (2024). Importance and Impact of New Digital Technologies on Business's Performance. Transformations in Business and Economics, 23(1), 62–85.

Seniutis, M., Gružauskas, V., Lileikiene, A., and Navickas, V. (2024). Conceptual framework for ethical artificial intelligence development in social services sector. Human Technology, 20(1), 6–24.

Sour, O., Maliki, S. B., and Benghalem, A. (2023). Modelling the Interconnection Between Technological Leadership and the Level of Use of Information and Communication Technologies. Business Ethics and Leadership, 7(3), 62–72.

The World Bank. (2023). Sovereign ESG Data Framework. Available at: https://esgdata.worldbank.org/data/framework?lang=en.

Wang, F., Jia, Y., Li, G., Monica, L., and Liu, Y. (2024). An Empirical Study of the Relationship Between Digital Transformation, Corporate Social Responsibility and Financial Performance. Business Ethics and Leadership, 8(1), 57–73.

Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. Health Economics and Management Review, 4(4), 17–27.

Yamin, T., and Murwaningsari, E. (2023). Exploring the Interplay Between Digital Technology, Transformational Leadership and Agility for Enhancing Organisational Performance. Business Ethics and Leadership, 7(4), 73–88.

Yarovenko, H., Lyeonov, S., Wojcieszek, K. A., and Szira, Z. (2023). Do IT users behave responsibly in terms of cybercrime protection? Human Technology, 19(2), 178–206.

Yin, H.-T., Wen, J., and Chang, C.-P. (2023). Going green with artificial intelligence: The path of technological change towards the renewable energy transition. Oeconomia Copernicana, 14(4), 1059–1095.

Zámek, D., and Zakharkina, Z. (2024). Research Trends in the Impact of Digitization and Transparency on National Security: Bibliometric Analysis. Financial Markets, Institutions and Risks, 8(1), 173–188.

Zatonatskiy, D., Leonov, S., Cieśliński, W., and Vasa, L. (2024). Determinants of global migration: The impact of ESG investments and foreign direct investment. Economics and Sociology, 17(1), 215–235.

Zvarikova, K., Dvorsky, J., Belas, J. J., and Metzker, Z. (2024). Model of sustainability of SMEs in V4 countries. Journal of Business Economics and Management, 25(2), 226–245.